

POSITIVE DENSITY OF INTEGER POLYNOMIALS WITH SOME PRESCRIBED PROPERTIES

ARTŪRAS DUBICKAS AND MIN SHA

ABSTRACT. In this paper, we show that various kinds of integer polynomials with prescribed properties of their roots have positive density. For example, we prove that almost all integer polynomials have exactly one or two roots with maximal modulus. We also show that for any positive integer n and any set of n distinct points symmetric with respect to the real line, there is a positive density of integer polynomials of degree n , height at most H and Galois group S_n whose roots are close to the given n points.

1. INTRODUCTION

The so-called *fundamental theorem of algebra*, first proved by Gauss, asserts that every non-constant univariate polynomial with complex coefficients has at least one complex root. Polynomials and various properties of their roots often play a crucial role in studying many mathematical objects.

For example, the properties of linear recurrence sequences (LRS) rely heavily on their characteristic polynomials. Recall that a LRS $\{u_n\}_{n=0}^\infty$ of order $n \geq 2$ with elements in \mathbb{C} is defined by the linear relation

$$u_{m+n} = a_1 u_{m+n-1} + \cdots + a_n u_m \quad (m = 0, 1, 2, \dots),$$

where $a_1, \dots, a_n \in \mathbb{C}$ (called the *coefficients*), $a_n \neq 0$ and $u_j \neq 0$ for at least one j in the range $0 \leq j \leq n-1$. The characteristic polynomial of this LRS is

$$f(X) = X^n - a_1 X^{n-1} - \cdots - a_n = \prod_{i=1}^n (X - \alpha_i) \in \mathbb{C}[X],$$

where all α_i are said to be the *characteristic roots* of the sequence $\{u_n\}_{n=0}^\infty$. The sequence $\{u_n\}_{n=0}^\infty$ is called *non-degenerate* if the quotient of any of its two distinct characteristic roots is not a root of unity. Then, there are only finitely many integers n with $u_n = 0$ if the sequence is

2010 *Mathematics Subject Classification.* Primary 11C08; Secondary 11B37.

Key words and phrases. Integer polynomial, dominant polynomial, polynomial root, positive density.

non-degenerate; otherwise, there may be infinitely many such integers. It has been proved in [11] that almost all LRS with integer (or rational) coefficients are non-degenerate.

In this paper, a polynomial is called *dominant* if it has a simple root (called *dominant root*) whose modulus is strictly greater than the moduli of its remaining roots. The LRS with dominant characteristic polynomial (called *dominant LRS*) are often much easier to deal with, especially when considering Diophantine properties of linear recurrence sequences.

In order to interpret the meanings of “almost all” and “positive density”, we introduce the following definition, which only shows the right way to comprehend “almost all” and “positive density”, but does not explain all their meanings in this paper. Given a proposition **P** related to integer polynomials, for integers $n \geq 1$ and $H \geq 1$, we define the set

$$\begin{aligned} \mathcal{P}_n(H) = \{f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X] : \\ |a_i| \leq H, i = 1, \dots, n\}. \end{aligned}$$

We say that **P** is true *for almost all* (or *with density tending to 1*) monic integer polynomials if for any integer $n \geq 1$ we have

$$\lim_{H \rightarrow \infty} \frac{|\{f \in \mathcal{P}_n(H) : \mathbf{P} \text{ is true for } f\}|}{|\mathcal{P}_n(H)|} = 1.$$

Throughout, we use $|T|$ to denote the cardinality of a finite set T . In addition, we say that **P** is true *with positive density* if for any integer $n \geq 1$ the following holds:

$$\limsup_{H \rightarrow \infty} \frac{|\{f \in \mathcal{P}_n(H) : \mathbf{P} \text{ is true for } f\}|}{|\mathcal{P}_n(H)|} > 0,$$

which is equivalent to the following

$$H^n \ll |\{f \in \mathcal{P}_n(H) : \mathbf{P} \text{ is true for } f\}| \ll H^n.$$

In the same way we will also handle all integer polynomials (not necessarily monic), where the term H^n will be replaced by H^{n+1} .

It has been shown in [12] that almost all monic integer polynomials are dominant [12, Theorem 1.1], but it is not true for general integer polynomials (not necessarily monic) [12, Theorem 1.4]. That is, not almost all integer polynomials (not necessarily monic) have a dominant root. Therefore, it is natural to ask which kind of integer polynomials we should add to the set of dominant integer polynomials to make their density tend to one. The answer is “those with exactly two maximal complex conjugate roots”. In Section 3, we show that almost all integer

polynomials have at most two roots with maximal modulus. Furthermore, unlike in the monic case, “at most two” cannot be replaced by “one” or “two”. In particular, this result has been used in [19] to show that for almost all LRS of algebraic numbers with rational coefficients, the *Skolem problem*, which is to determine whether a given LRS has a zero term, is decidable with an explicit complexity. Besides, the result also gives a strong evidence that at least half of integer polynomials are dominant.

More precisely, put $A_n^*(k, H)$ for the cardinality of the set of integer polynomials of degree n and height at most H with exactly k roots of maximal modulus. The next theorem shows that the proportion of polynomials with at most two roots of maximal modulus ($A_n^*(1, H) + A_n^*(2, H)$) among all integer polynomials of degree n and height at most H (there are $2H(2H+1)^n$ of them) tends to 1 as $H \rightarrow \infty$. Namely,

Theorem 1.1. *For any integer $n \geq 2$, we have*

$$\lim_{H \rightarrow \infty} \frac{A_n^*(1, H) + A_n^*(2, H)}{2H(2H+1)^n} = 1.$$

Although it has been proved in [12] that almost all monic integer polynomials are dominant, in Section 3 we will also determine the growth rate of such monic integer polynomials with more than one root of maximal modulus. Theorem 1.1 will be derived from Theorem 3.4 which estimates the difference between the quantities $2H(2H+1)^n$ and $A_n^*(1, H) + A_n^*(2, H)$.

As an another example, let us consider number fields. Let K be a number field of degree $n \geq 2$ and generated by α over \mathbb{Q} , and let f be the minimal integer polynomial of α over \mathbb{Z} . If f has exactly r real roots and $2s$ non-real roots ($r \geq 0, s \geq 0$), then it is well known that there are $r+s$ non-isomorphic embeddings of K into \mathbb{C} (r real embeddings and s complex embeddings), and the rank of the unit group of the ring of integers of K is $r+s-1$ (by Dirichlet’s unit theorem). So, for two given non-negative integers r, s with $n = r+2s \geq 2$, one may investigate the proportion of number fields of degree n with exactly r real embeddings and s complex embeddings. We will investigate this problem in the setting of integer polynomials. In Section 4 we will show that various kinds of integer polynomials with prescribed locations of their roots have positive density; for instance, integer polynomials of degree n with exactly r real roots and $2s$ non-real roots, where $r+2s = n$. In some sense, these results suggest that there are quite many number fields with arbitrary real and complex embeddings and, in particular, their density is positive.

More precisely, for positive integers n, H and non-negative integers r, s with $n = r + 2s$, let us define the set

$$\mathcal{D}_n^*(r, s; H) = \{f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X] : H(f) \leq H, \\ a_0 \neq 0, f \text{ has exactly } r \text{ real roots and } 2s \text{ non-real roots}\}.$$

Then, put $D_n^*(r, s; H) = |\mathcal{D}_n^*(r, s; H)|$. The following result asserts that there are many integer polynomials of degree n , which have r real roots and $2s$ non-real roots, where $r + 2s = n$.

Theorem 1.2. *For any integers $n, H \geq 1$ and any non-negative integers r, s such that $n = r + 2s$, we have*

$$H^{n+1} \ll D_n^*(r, s; H) \ll H^{n+1}.$$

Recall that van der Waerden [20] showed that, for almost all integer polynomials of degree $n \geq 1$, the Galois group of their splitting fields over \mathbb{Q} is the full symmetric group S_n . Theorem 1.2 implies that various placings of roots are possible for generic polynomials with Galois group S_n .

Theorem 1.2 is an immediate corollary of the following more general result:

Theorem 1.3. *Let S be a set of n distinct points β_1, \dots, β_n in the complex plane \mathbb{C} symmetric with respect to the real line, i. e.*

$$S = \{\beta_1, \dots, \beta_n\} = \{\overline{\beta_1}, \dots, \overline{\beta_n}\}.$$

Then, for each sufficiently small positive number ε , there exists a constant $C = C(\varepsilon, S) > 0$ such that the number of integer polynomials f of degree n and height at most H with Galois group S_n and n roots lying ε -neighbourhoods of β_1, \dots, β_n respectively (and, in addition, such that the root of each such f lying in the open disc $|z - \beta_i| < \varepsilon$ is real if and only if the number β_i is real) is at least CH^{n+1} .

In some sense Theorem 1.3 is a non-monic version of an old theorem of Motzkin [18]; see also [9].

We also want to compare our results with a related result of Akiyama and Pethő [2] (see also their previous paper [1]). Let $M_n(r, s; T)$ be the number of monic integer polynomials of degree n and having exactly r real roots and $2s$ non-real roots such that the maximal modulus of the roots is less than T . In [2, Theorem 3.1], it has been proved that

$$(1.1) \quad |M_n(r, s; T) - v_n^{(s)} T^{n(n+1)/2}| \leq c_1 T^{n(n+1)/2-1},$$

where $v_n^{(s)}$ is some quantity defined in [2, Section 2], and c_1 is a constant depending only on n and s . This result suggests that such monic

integer polynomials have positive density among all the monic integer polynomials. So, in some sense Theorem 1.2 generalizes the result to the case of general integer polynomials (not necessarily monic). It would be of interest to obtain an asymptotic formula as (1.1) in our setting as well.

Throughout the paper, we use the Landau symbol O and the Vinogradov symbol \ll . Recall that the assertions $U = O(V)$ and $U \ll V$ (sometimes we will write this also as $V \gg U$) are both equivalent to the inequality $|U| \leq cV$ with some constant $c > 0$. In this paper, the constants implied in the symbols O, \ll and in the phrase “up to some constant” only possibly depend on the degree n . Besides, we always assume that H is a positive integer (greater than 1 if there is the factor $\log H$ in the corresponding formula), and n is a positive integer.

The proofs come from several sources. Some preliminary results and our main lemmas (Lemma 2.6 and Lemma 2.7) are given in the next section. The proof of some results related to Theorem 1.1 and several similar results are given in Section 3 which is concluded with two proofs of Theorem 1.1 itself. The proof of Theorem 1.3 is given at the beginning of Section 4. The lower bounds usually come from some series of explicit examples (monic case) and from Lemma 2.6 (non-monic case).

2. PRELIMINARIES

In this section, for the convenience of the reader we gather some definitions and give some results which will be used later on.

2.1. Some useful results about polynomials.

Given a polynomial

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n = a_0(X - \alpha_1) \cdots (X - \alpha_n) \in \mathbb{C}[X]$$

of degree $n \geq 1$, we assume that the roots $\alpha_1, \dots, \alpha_n$ (listed with multiplicities) are labelled so that $|\alpha_1| \geq |\alpha_2| \geq \cdots \geq |\alpha_n|$. In case $|\alpha_1| = \cdots = |\alpha_k| > |\alpha_{k+1}|$, we say that f has *exactly k roots with maximal modulus*.

For the above polynomial $f(X)$, its *height* is defined by

$$H(f) = \max_{0 \leq j \leq n} |a_j|,$$

and its *Mahler measure* by

$$M(f) = |a_0| \prod_{j=1}^n \max\{1, |\alpha_j|\}.$$

These two quantities are related by the following well-known inequality

$$(2.1) \quad 2^{-n}H(f) \leq M(f) \leq \sqrt{n+1}H(f),$$

for instance, see [21, (3.12)].

There are various bounds on the moduli of roots of polynomials. Here, we use the one due to Fujiwara [14]; for a reference in English see [3].

Lemma 2.1. *Given a polynomial $f(X) = a_0X^n + \dots + a_n \in \mathbb{C}[X]$ of degree $n \geq 1$, the moduli of all its roots do not exceed*

$$2 \max \left\{ \left| \frac{a_1}{a_0} \right|, \left| \frac{a_2}{a_0} \right|^{1/2}, \dots, \left| \frac{a_{n-1}}{a_0} \right|^{1/(n-1)}, \left| \frac{a_n}{2a_0} \right|^{1/n} \right\}.$$

The following result was obtained by Ferguson [13]; see also a previous result of Boyd [4].

Lemma 2.2. *If $f \in \mathbb{Z}[X]$ is an irreducible polynomial which has exactly m roots on a circle $|z| = c > 0$, at least one of which is real, then one has $f(X) = g(X^m)$, where the polynomial $g \in \mathbb{Z}[X]$ has at most one real root on any circle in the plane with center at the origin.*

It is well known that the roots of a polynomial depend continuously on its coefficients. Here, we essentially quote an explicit version about this continuous dependence from [17, Theorem 1.4].

Lemma 2.3. *Let $f, g \in \mathbb{C}[X]$ of degree $n \geq 1$ be as follows:*

$$f(X) = a_0X^n + a_1X^{n-1} + \dots + a_n = a_0 \prod_{i=1}^m (X - \alpha_i)^{e_i},$$

$$g(X) = (a_0 + \epsilon_0)X^n + (a_1 + \epsilon_1)X^{n-1} + \dots + (a_n + \epsilon_n),$$

where $\alpha_1, \dots, \alpha_m$ are distinct roots of f , and $e_1 + \dots + e_m = n$. Let

$$0 < \gamma < \frac{1}{2} \min_{i \neq j} |\alpha_i - \alpha_j|, \quad M = \max_{1 \leq j \leq m} \left\{ \sum_{i=0}^n (\gamma + |\alpha_j|)^i \right\},$$

$$\delta = \min_{1 \leq j \leq m} \left\{ |a_0| \gamma^{e_j} \prod_{i=1, i \neq j}^m (|\alpha_i - \alpha_j| - \gamma)^{e_i} \right\}.$$

(Note that if $e_1 = n$, then γ can be chosen as an arbitrary positive real number, and $\delta = |a_0| \gamma^{e_1}$.) Choose a real number $\epsilon = \delta/M$, and assume that $|\epsilon_i| < \epsilon$ for any $0 \leq i \leq n$. Then, g has precisely e_j zeros in the disk D_j with center at α_j and radius γ for each $1 \leq j \leq m$ (counted with multiplicity).

Proof. Let

$$h(X) = \epsilon_0 X^n + \epsilon_1 X^{n-1} + \cdots + \epsilon_n.$$

Then, $g = f + h$. Fix an integer j with $1 \leq j \leq m$. Pick an arbitrary point x on the boundary of D_j , clearly we have $|h(x)| < \epsilon M$. Besides,

$$|f(x)| \geq |a_0| \gamma^{e_j} \prod_{i=1, i \neq j}^m (|\alpha_i - \alpha_j| - \gamma)^{e_i} \geq \delta.$$

Since $\delta = \epsilon M$, on the boundary of D_j we always have $|h(x)| < |f(x)|$. By Rouché's theorem, this means that g has the same number of zeros in D_j as does f . Note that f has only one root α_j in D_j with multiplicity e_j . Thus, the polynomial g has precisely e_j zeros in the disk D_j . \square

Let $\rho_m(n, H)$ be the number of monic polynomials

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X], \quad n \geq 2, \quad H(f) \leq H,$$

which are reducible in $\mathbb{Z}[X]$ with an irreducible factor of degree m , $1 \leq m \leq n/2$. In [20], van der Waerden proved the following sharp lower and upper bounds for $\rho_m(n, H)$; see also [5] for a reference in English.

Lemma 2.4. *For integers $n \geq 2$ and $m \geq 1$, we have*

$$H^{n-m} \ll \rho_m(n, H) \ll H^{n-m} \quad \text{if } 1 \leq m < n/2,$$

$$H^{n-m} \log H \ll \rho_m(n, H) \ll H^{n-m} \log H \quad \text{if } m = n/2.$$

Similarly, if $\rho_m^*(n, H)$ is the number of polynomials

$$f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X], \quad a_0 \neq 0, n \geq 2,$$

which are reducible in $\mathbb{Z}[X]$ with an irreducible factor of degree m , $1 \leq m < n/2$, and satisfy $H(f) \leq H$, then, Kuba [16, Theorems 1 and 4] (see also [10]) showed that

Lemma 2.5. *For integers $n \geq 3$ and $m \geq 1$, we have*

$$H^{n-m+1} \ll \rho_m^*(n, H) \ll H^{n-m+1} \quad \text{if } 1 \leq m < n/2.$$

Furthermore, the number of reducible integer polynomials of degree $n \geq 3$ and height at most H is $O(H^n)$ and of degree $n = 2$ and height at most H is $O(H^2 \log H)$.

2.2. An estimate of polynomials with roots close to the roots of a real polynomial. In the case of general (not monic) polynomials the next lemma will be used in a number of estimates from below.

Lemma 2.6. *Given a separable polynomial*

$$h(X) = b_0 X^n + b_1 X^{n-1} + \cdots + b_n \in \mathbb{R}[X]$$

of degree $n \geq 1$ with roots β_1, \dots, β_n and a sufficiently small positive number ε , there exists a constant $C = C(\varepsilon, h)$ such that the number of integer polynomials f of degree n and height at most H with n roots lying ε -neighbourhoods of β_1, \dots, β_n respectively (and such that the root of each such f lying in the open disc $|z - \beta_i| < \varepsilon$ is real if and only if the number β_i is real) is at least CH^{n+1} .

Proof. Suppose that the polynomial $h(X)$ has exactly r real roots β_1, \dots, β_r and $2s$ non-real roots $\beta_{r+1}, \dots, \beta_n$. These occur as complex conjugate pairs $\beta_{r+2i} = \overline{\beta_{r+2i-1}}$ for $i = 1, \dots, (n-r)/2$. By Lemma 2.3, there exist two positive real numbers γ, ϵ depending only on h such that any polynomial

$$(2.2) \quad g(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{R}[X]$$

with $|a_i - b_i| < \epsilon$ for any $0 \leq i \leq n$ has exactly one root in the disk D_j with center at β_j and radius γ for each $1 \leq j \leq n$.

For any $r+1 \leq j \leq n$, since there are no real numbers in D_j , the root of g located in D_j must be non-real. Fix j in the range $1 \leq j \leq r$. If the root of g located in D_j is non-real, then its complex conjugate is also located in D_j , so g has at least two distinct roots in D_j . This leads to a contradiction. Thus, g has exactly r real roots and $2s$ non-real roots.

For any $0 \leq i \leq n$, denote by I_i the open interval $(H(b_i - \epsilon), H(b_i + \epsilon))$. Consider a polynomial

$$(2.3) \quad f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$$

with $a_i \in I_i$ for any $0 \leq i \leq n$. Then $f(X)/H$ is the polynomial of type (2.2), so f has exactly r real roots and $2s$ non-real roots in the discs $|z - \beta_j| < \gamma$, $j = 1, \dots, n$. Note that there are at least $\lfloor 2\epsilon H \rfloor^{n+1} \gg H^{n+1}$ of such integer polynomials f which have the form (2.3). Their heights satisfy $H(f) \ll H$. For sufficiently large H , since all the implied constants depend on h, γ and ϵ but are independent of H , we deduce the lower bound CH^{n+1} , as claimed. \square

2.3. An estimate of polynomials with a multiplicative relation among its roots. For further applications, we need to count a special

kind of integer polynomials whose roots satisfy some multiplicative relation.

Lemma 2.7. *For integers $n \geq 4$ and $H \geq 1$, we have*

$$|\{f \in \mathbb{Z}[X] : \deg f = n, H(f) \leq H, f \text{ is monic and has four roots } \alpha_1, \alpha_2, \alpha_3, \alpha_4 \text{ such that } \alpha_1\alpha_2 = \alpha_3\alpha_4\}| \ll H^{n-1},$$

and

$$|\{f \in \mathbb{Z}[X] : \deg f = n, H(f) \leq H, f \text{ has four roots } \alpha_1, \alpha_2, \alpha_3, \alpha_4 \text{ such that } \alpha_1\alpha_2 = \alpha_3\alpha_4\}| \ll H^n.$$

Proof. The proofs of these two upper bounds are the same. Here, for brevity we only prove the second upper bound. Write

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n = a_0 \prod_{i=1}^n (X - \alpha_i).$$

Here, although f may have multiple roots, we still view that all $\alpha_1, \dots, \alpha_n$ are different (at least from the viewpoint of symbols). For integer k in the range $1 \leq k \leq n$, the k th elementary symmetric polynomial with respect to $\alpha_1, \dots, \alpha_n$ is

$$s_k(\alpha_1, \dots, \alpha_n) = \sum_{1 \leq j_1 < j_2 < \cdots < j_k \leq n} \alpha_{j_1} \alpha_{j_2} \cdots \alpha_{j_k} = (-1)^k \frac{a_k}{a_0}.$$

Consider the polynomial

$$\prod_{1 \leq i < j \leq n} (X - \alpha_i \alpha_j).$$

Its coefficients are symmetric polynomials with respect to $\alpha_1, \dots, \alpha_n$ over \mathbb{Z} , so they are integer polynomials in the variables $a_1/a_0, \dots, a_n/a_0$ (in fact, the integer coefficients depend only on n). So, multiplied by an appropriate power of a_0 (depending only on n), this product is an integer polynomial, say $g(X)$, whose coefficients are polynomials with integer coefficients in a_0, a_1, \dots, a_n . Let Δ be the discriminant of the polynomial g . Then, Δ is a polynomial in a_0, a_1, \dots, a_n with integer coefficients (depending only on n). The property $\alpha_1\alpha_2 = \alpha_3\alpha_4$ implies that $\Delta = 0$. So one of the coefficients a_0, a_1, \dots, a_n , say a_0 , is predetermined in $m = \deg_{a_0} \Delta$ ways by other n coefficients a_1, \dots, a_n (note that the degree of the polynomial Δ , which is not less than m , depends only on n). Consequently, the number of such polynomials f is $O(H^n)$. \square

2.4. Probabilistic Galois Theory. In Section 3, we will present an alternative proof of Theorem 1.1, by using Probabilistic Galois Theory. Here are some basic facts concerning it.

Let S_n be the full symmetric group on a finite set of n symbols. Given a polynomial $f \in \mathbb{Z}[X]$, denote by G_f the Galois group of the splitting field of f over \mathbb{Q} . For any integers $n \geq 1$ and $H \geq 1$, we define the sets

$$\begin{aligned} \mathcal{E}_n(H) = \{f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X] : \\ G_f \neq S_n, |a_i| \leq H, i = 1, 2, \dots, n\}, \end{aligned}$$

and

$$\begin{aligned} \mathcal{E}_n^*(H) = \{f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X] : \\ G_f \neq S_n, a_0 \neq 0, |a_i| \leq H, i = 0, 1, \dots, n\}. \end{aligned}$$

Then, put $E_n(H) = |\mathcal{E}_n(H)|$ and $E_n^*(H) = |\mathcal{E}_n^*(H)|$.

The study of bounding $E_n(H)$ and $E_n^*(H)$ was initiated by van der Waerden [20] who showed that

Lemma 2.8. *For integers $n \geq 3$ and $H \geq 2$, we have*

$$E_n(H) \ll H^{n-1/(6(n-2) \log \log H)}$$

and

$$E_n^*(H) \ll H^{n+1-1/(6(n-2) \log \log H)},$$

where the implied constants depend only on n .

Later, the bound on $E_n(H)$ has been improved in several ways; see [6, 7, 8, 15]. For instance, Gallagher [15] proved that $E_n(H) \ll H^{n-1/2} \log H$, and recently Zywina improved this bound to $E_n(H) \ll H^{n-1/2}$ in [22, Proposition 1.5].

3. COUNTING INTEGER POLYNOMIALS VIA MODULI OF THEIR ROOTS

In [12, Theorem 1.1], it has been shown that almost all monic integer polynomials are dominant (that is, have exactly one root with maximal modulus). Here, our considerations include both monic and general integer polynomials.

For positive integers n, k with $k \leq n$, we define the sets

$$\begin{aligned} \mathcal{A}_n(k, H) = \{f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X] : H(f) \leq H, \\ f \text{ has exactly } k \text{ roots with maximal modulus}\}, \end{aligned}$$

and

$$\mathcal{A}_n^*(k, H) = \{f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X] : H(f) \leq H, \\ a_0 \neq 0, f \text{ has exactly } k \text{ roots with maximal modulus}\}.$$

Then, denote $A_n(k, H) = |\mathcal{A}_n(k, H)|$ and $A_n^*(k, H) = |\mathcal{A}_n^*(k, H)|$.

In this section, we will estimate $A_n(k, H)$ and $A_n^*(k, H)$.

3.1. The monic case. It has been proved in [12, Theorem 1.1] that

$$\lim_{H \rightarrow \infty} \frac{A_n(1, H)}{(2H+1)^n} = 1.$$

Now, we estimate the error term, that is, the difference between the quantities $A_n(1, H)$ and $(2H+1)^n$.

Theorem 3.1. *For integers $n \geq 2$ and $H \geq 1$, we have*

$$H^{n-1/2} \ll (2H+1)^n - A_n(1, H) = \sum_{k=2}^n A_n(k, H) \ll H^{n-1/2}.$$

Proof. First, given an arbitrary polynomial $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{C}[X]$, let R be the maximal modulus of the roots of f . Suppose that f does not have exactly one root with maximal modulus, that is, it has at least two roots on the circle $|z| = R$. Then, by the definition of the Mahler measure, we have $R^2 \leq M(f)$. Noticing that $|a_1| \leq nR$ and applying (2.1), we obtain

$$|a_1| \leq n(n+1)^{1/4} H(f)^{1/2},$$

which implies that

$$\sum_{k=2}^n A_n(k, H) \ll H^{n-1/2},$$

since $|a_2|, \dots, |a_n| \leq H$.

For a lower bound, let us consider the following polynomials

$$f(X) = X^n + a_1 X^{n-1} + a_2 X^{n-2} + \cdots + a_n \in \mathbb{Z}[X],$$

where $-\delta\sqrt{H} \leq a_1 < 0$ for some fixed real number $0 < \delta < 1$ and $1 \leq a_i \leq H$ for each $2 \leq i \leq n$ and $a_2 \geq \delta^2 H$, and either $a_2 \geq a_3, a_4 \geq a_5, \dots, a_{n-2} \geq a_{n-1}$ if n is even, or $a_2 \geq a_3, a_4 \geq a_5, \dots, a_{n-1} \geq a_n$ if n is odd. Then, when H is large enough, such polynomials f indeed exist, and we further claim that $f \notin \mathcal{A}_n(1, H)$. It is clear that, by counting these polynomials f , we would get

$$H^{n-1/2} \ll \sum_{k=2}^n A_n(k, H),$$

which completes the proof.

To prove the claim it suffices to show that the largest in modulus root of f is non-real. Assume that f has a real root $x \geq 0$. Clearly, $x > 0$. Since $a_2, \dots, a_n > 0$, we have

$$f(x) > x^{n-1}(x + a_1) \geq 0$$

if $x \geq |a_1|$, so we must have $0 < x < |a_1|$. Thus, $|a_1x| < |a_1|^2 \leq \delta^2 H$. Then

$$f(x) > a_1x^{n-1} + a_2x^{n-2} = x^{n-2}(a_1x + a_2) > 0,$$

which contradicts $f(x) = 0$. So, f does not have non-negative roots.

Set $g(X) = f(-X)$ if n is even, otherwise let $g(X) = -f(-X)$. Then, the negative real roots of $f(X)$ are exactly the positive real roots of $g(X)$. In case n is even, as

$$g(X) = X^n - a_1X^{n-1} + a_2X^{n-2} - a_3X^{n-3} + \dots + a_{n-2}X^2 - a_{n-1}X + a_n,$$

for any real $x \geq 1$ we have

$$g(x) > x^{n-3}(a_2x - a_3) + \dots + x(a_{n-2}x - a_{n-1}) \geq 0.$$

(Evidently, for $n = 2$ the polynomial $g(X)$ has no positive roots.) Similarly, if n is odd, observe that

$$g(X) = X^n - a_1X^{n-1} + a_2X^{n-2} - a_3X^{n-3} + \dots + a_{n-1}X - a_n,$$

so for any real $x \geq 1$ we have

$$g(x) > x^{n-3}(a_2x - a_3) + \dots + (a_{n-1}x - a_n) \geq 0.$$

Therefore, all the real roots of $f(X)$ (if any) lie in the interval $(-1, 0)$.

Moreover, writing f as $f(X) = \prod_{i=1}^n (X - \alpha_i)$, we obtain $a_n = (-1)^n \prod_{i=1}^n \alpha_i$. Since $a_n \geq 1$, we see that $|\alpha_i| \geq 1$ for at least one index i . So, not all the roots of $f(X)$ lie strictly inside the unit circle. It follows that the largest in modulus root of f is non-real, and hence $f \notin \mathcal{A}_n(1, H)$. \square

We remark that for the polynomial f constructed in the second part of the above proof, some extra conditions can be added to make sure that f only has non-real roots when n is even. For example, if $n \geq 4$ is even, we can further assume that

$$\min_{1 \leq i \leq n/2} a_{2i} \geq \max_{1 \leq i \leq (n-2)/2} a_{2i+1}.$$

Then, for any $0 < x < 1$, we have

$$\begin{aligned} g(x) &= x^n - a_1x^{n-1} + a_2x^{n-2} + x^{n-4}(a_4 - a_3x) + \dots + (a_n - a_{n-1}x) \\ &> x^n - a_1x^{n-1} + a_2x^{n-2} > 0, \end{aligned}$$

which implies that f has no roots in the interval $(-1, 0)$. Thus, f indeed has no real roots.

The next theorem shows that the main contribution in the sum $\sum_{k=2}^n A_n(k, H)$ considered in Theorem 3.1 comes from $A_n(2, H)$.

Theorem 3.2. *For integers $n \geq 3$ and $H \geq 1$, we have*

$$\sum_{k=3}^n A_n(k, H) \ll H^{n-1}.$$

Proof. We choose an arbitrary polynomial $f \in \bigcup_{k=3}^n \mathcal{A}_n(k, H)$. Suppose first that f is reducible. Then, it follows directly from Lemma 2.4 that the number of these polynomials f is $O(H^{n-1})$.

Next, suppose that f is irreducible. If f has a real root with maximal modulus (for instance, when k is odd), then by Lemma 2.2, we know that $f(X) = g(X^k)$ for some $g \in \mathbb{Z}[X]$. So, the number of such polynomials f is bounded above by

$$\sum_{k=3}^n (2H+1)^{n/k} \leq (n-2)(2H+1)^{n/3} \ll H^{n-2}.$$

Finally, assume that f has no real roots with maximal modulus, but has at least three roots of maximal modulus. Then, we must have $n \geq 4$, and so there are at least two pairs of complex conjugate (non-real) roots with maximal modulus, say, the pair $\alpha_1 = \alpha, \alpha_2 = \overline{\alpha}$ and another pair $\alpha_3 = \beta, \alpha_4 = \overline{\beta}$. Clearly, we have

$$\alpha_1\alpha_2 = \alpha_3\alpha_4,$$

and so the desired result follows from Lemma 2.7. \square

Combining Theorems 3.1 and 3.2 we conclude that

Corollary 3.3. *For integers $n \geq 2$ and $H \geq 1$, we have*

$$H^{n-1/2} \ll A_n(2, H) \ll H^{n-1/2}.$$

3.2. The non-monic case. In [12, Theorem 1.4], it has been shown that for any integer $n \geq 2$ we have

$$\liminf_{H \rightarrow \infty} \frac{A_n^*(1, H)}{(2H)^{n+1}} \geq \frac{1}{3n^2\sqrt{n+1}}$$

and

$$\limsup_{H \rightarrow \infty} \frac{A_n^*(1, H)}{(2H)^{n+1}} \leq \begin{cases} 1 - 1/(3 \cdot 2^{3n/2-1}) & \text{if } n \text{ is even,} \\ 1 - 1/(3 \cdot 2^{(3n+1)/2}) & \text{if } n \text{ is odd.} \end{cases}$$

The above two bounds say that the density of dominant integer polynomials is positive but does not tend to 1 as $H \rightarrow \infty$. Moreover, it has been conjectured in [12] that

$$(3.1) \quad \limsup_{H \rightarrow \infty} \frac{A_n^*(1, H)}{(2H)^{n+1}} > \frac{1}{2},$$

which means that at least half of integer polynomials are dominant.

In this section, we show that almost all integer polynomials have exactly one or two roots with maximal modulus, and we also provide a strong evidence for the validity of (3.1).

The following result implies that the density of integer polynomials with more than two roots of maximal modulus tends to zero as $H \rightarrow \infty$. (It can be viewed as a non-monic version of Theorem 3.2.)

Theorem 3.4. *For integers $n \geq 3$ and $H \geq 1$, we have*

$$\sum_{k=3}^n A_n^*(k, H) \ll H^n.$$

Proof. Since the number of reducible integer polynomials of degree $n \geq 3$ and height at most H is $O(H^n)$ (see, for example, Lemma 2.5), we only need to consider those polynomials contained in $\mathcal{A}_n^*(k, H)$ that are irreducible. In the rest of the proof, let $f \in \mathcal{A}_n^*(k, H)$ be an irreducible polynomial.

If f has a real root with maximal modulus (for instance, when k is odd), then by Lemma 2.2, we know that $f(X) = g(X^k)$ for some $g \in \mathbb{Z}[X]$. So, the number of such polynomials f is bounded above by

$$\sum_{k=3}^n (2H+1)^{n/k+1} \leq (n-2)(2H+1)^{n/3+1} \ll H^{n-1}.$$

Now suppose that f has no real roots with maximal modulus. Then, we must have $n \geq 4$, and there are at least two pairs of complex conjugate (non-real) roots with maximal modulus, say, the pair $\alpha_1 = \alpha, \alpha_2 = \bar{\alpha}$ and another pair $\alpha_3 = \beta, \alpha_4 = \bar{\beta}$. Now, as above we have $\alpha_1\alpha_2 = \alpha_3\alpha_4$, and so the desired result follows from Lemma 2.7. \square

By considering the polynomials $a_0X^3 + a_3$, we have $A_3^*(3, H) \gg H^2$. As an example of a lower bound we will also show that

$$A_n^*(3, H) \gg H^{n-2}$$

for any integer $n \geq 4$. Indeed, consider the polynomials

$$f(X) = (X^3 + 8)(a_0X^{n-3} + \cdots + a_{n-4}X + a_{n-3}) \in \mathbb{Z}[X],$$

where $\lambda_1 H < a_0 < \lambda_2 H$, $\delta_1 H < a_i < \delta_2 H$ for $1 \leq i \leq n-3$, and $0 < \delta_1 < \delta_2 < \lambda_1 < \lambda_2 \leq 1/9$. Clearly, $H(f) \leq H$. Using Lemma 2.1, we know that the moduli of all the roots of the polynomial $a_0 X^{n-3} + \cdots + a_{n-4} X + a_{n-3}$ are less than 2. So, $f \in \mathcal{A}_n^*(3, H)$. Thus, counting those polynomials f we obtain the lower bound $A_n^*(3, H) \gg H^{n-2}$.

Theorem 3.4 implies Theorem 1.1 asserting that almost all integer polynomials have exactly one or two roots with maximal modulus. Indeed, the number of integer polynomials of degree $n \geq 1$ and height at most $H \geq 1$ is exactly $2H(2H+1)^n = \sum_{k=1}^n A_n^*(k, H)$. Thus, Theorem 1.1 follows directly from Theorem 3.4.

In the sequel, we use the so-called Probabilistic Galois Theory to give an alternative proof of Theorem 1.1, which, although gives weaker estimate on the error term, might be of some interest as well. All we need to do is to show that for any $3 \leq k \leq n$, we have

$$\lim_{H \rightarrow \infty} \frac{A_n^*(k, H)}{H^{n+1}} = 0.$$

Now, assume that $3 \leq k \leq n$. In fact, since the number of reducible integer polynomials of degree $n \geq 3$ and height at most H is $O(H^n)$ (for example, see Lemma 2.5), we only need to consider those polynomials contained in $\mathcal{A}_n^*(k, H)$ that are irreducible.

Let $f \in \mathcal{A}_n^*(k, H)$ be an irreducible polynomial. If f has a real root with maximal modulus, then by Lemma 2.2, we know that $f(X) = g(X^k)$ for some $g \in \mathbb{Z}[X]$; so, the number of such polynomials f is $O(H^{n/k+1})$.

Now suppose that f has no real roots with maximal modulus. Then, there are at least two pairs of complex conjugate (non-real) roots with maximal modulus, say, the pair $\alpha_1 = \alpha, \alpha_2 = \bar{\alpha}$ and another pair $\alpha_3 = \beta, \alpha_4 = \bar{\beta}$. In particular, this yields $n \geq 4$. Clearly, we have

$$(3.2) \quad \alpha_1 \alpha_2 = \alpha_3 \alpha_4.$$

We claim that $f \in \mathcal{E}_n^*(H)$, where $n \geq 4$.

Assume that $f \notin \mathcal{E}_n^*(H)$. Then, the Galois group of f is S_n , so there exists an embedding σ such that

$$\sigma(\alpha_1) = \alpha_3, \sigma(\alpha_2) = \alpha_2, \sigma(\alpha_3) = \alpha_1, \sigma(\alpha_4) = \alpha_4.$$

Together with (3.2), we get $\alpha_3 \alpha_2 = \alpha_1 \alpha_4$, and so $\alpha_1 \alpha_3 \alpha_2^2 = \alpha_1 \alpha_3 \alpha_4^2$. Thus, we find that $\alpha_2^2 = \alpha_4^2$, so $\alpha_2 = -\alpha_4$. By a similar argument (interchanging α_1 with α_4), we find that $\alpha_2 = -\alpha_3$. So, we obtain $\alpha_3 = \alpha_4$, which is a contradiction. Thus, we must have $f \in \mathcal{E}_n^*(H)$. Therefore, the desired result follows from Lemma 2.8.

4. COUNTING INTEGER POLYNOMIALS VIA THE LOCATIONS OF THEIR ROOTS

In this section, we begin with the proof of Theorem 1.3 asserting that integer polynomials with various locations of their roots have positive density. It suffices to prove the lower bound. But the lower bound follows from Lemma 2.6, where

$$h(X) = (X - \beta_1) \cdots (X - \beta_n) \in \mathbb{R}[X]$$

is a separable monic polynomial, combined with the second inequality of Lemma 2.8. (For $n = 2$, all irreducible polynomials have the Galois group S_2 , so the result follows from Lemma 2.5.)

In conclusion, we remark that, since it is likely that $A_n^*(1, H) > A_n^*(2, H)$, Theorem 1.1 provides a strong evidence that the conjecture (3.1) may be true. It also naturally implies the following approach. Notice that for any polynomial having only non-zero roots, a root with maximal (resp. minimal) modulus corresponds to a root with minimal (resp. maximal) modulus of its reciprocal polynomial. So regarding Theorem 1.1, we can only consider integer polynomials with exactly m_1 roots of minimal modulus and exactly m_2 roots of maximal modulus, where $m_1, m_2 \in \{1, 2\}$. For integers $n \geq 1, H \geq 1$ and $m_1, m_2 \in \{1, 2\}$, let $\mathcal{B}_n^*(m_1, m_2; H)$ be the set of such integer polynomials of degree n and height at most H , and set

$$B_n^*(m_1, m_2; H) = |\mathcal{B}_n^*(m_1, m_2; H)|.$$

Now, Theorem 1.1 can be restated as

$$\lim_{H \rightarrow \infty} \frac{B_n^*(1, 1; H) + B_n^*(2, 1; H) + B_n^*(1, 2; H) + B_n^*(2, 2; H)}{2H(2H+1)^n} = 1$$

for any integer $n \geq 2$.

Using reciprocal polynomials, it is easy to see that $B_n^*(2, 1; H) = B_n^*(1, 2; H)$. So, if one could prove that $B_n^*(1, 1; H) > B_n^*(2, 2; H)$ (it is likely to be true), then the conjecture (3.1) would be established.

For $n = 3$ the conjecture is true, since $B_3^*(2, 2; H) = 0$. But in general, it is not easy to compare $B_n^*(1, 1; H)$ with $B_n^*(2, 2; H)$. The following result implies that, for $n \geq 4$, the growth rate of each of the four quantities $B_n^*(m_1, m_2; H)$ is H^{n+1} with respect to H .

Theorem 4.1. *For integers $n \geq 3$ and $H \geq 1$, we have*

$$H^{n+1} \ll B_n^*(1, 1; H) \ll H^{n+1},$$

$$H^{n+1} \ll B_n^*(2, 1; H) \ll H^{n+1},$$

$$H^{n+1} \ll B_n^*(1, 2; H) \ll H^{n+1}.$$

Furthermore, for integers $n \geq 4$ and $H \geq 1$, we have

$$H^{n+1} \ll B_n^*(2, 2; H) \ll H^{n+1}.$$

Proof. All upper bounds are trivial. The lower bounds follow from Theorem 1.3. Indeed, for instance, in order to get the last lower bound we can consider the polynomial $h(X) = (X^2+1)(X^2+5)(X^{n-4}+2^{n-4})$. The polynomials $f \in \mathbb{Z}[X]$ described in Lemma 2.6 will then be in the set $B_n^*(2, 2; H)$, because their roots close to $\pm\sqrt{-1}$ will be conjugate complex numbers (with minimal modulus) and also their roots close to $\pm\sqrt{-5}$ will be conjugate complex numbers (with maximal modulus), whereas the remaining $n-4$ roots will have the moduli close to 2. \square

ACKNOWLEDGEMENTS

The authors are very grateful to the referee for useful comments and suggestions. They would like to thank Yuri Bilu for explaining the result in [20] to them. They also want to thank Igor E. Shparlinski and Manas Patra for useful discussions and helpful comments. The second author appreciates Wuxing Cai's valuable comments when he gave a talk on part of this paper at South China University of Technology. The research of M. S. was supported by the Australian Research Council Grant DP130100237.

REFERENCES

- [1] S. Akiyama and A. Pethő, *On the distribution of polynomials with bounded roots, I. Polynomials with real coefficients*, J. Math. Soc. Japan **66** (2014), 1–23.
- [2] S. Akiyama and A. Pethő, *The distribution of polynomials with bounded roots, II. Polynomials with integer coefficients*, Uniform Distribution Theory **9** (2014), 5–19.
- [3] P. Batra, *A property of nearly optimal root-bound*, J. Comput. Appl. Math. **167** (2004), 489–491.
- [4] D. W. Boyd, *Irreducible polynomials with many roots of maximal modulus*, Acta Arith. **68** (1994), 85–88.
- [5] R. Chela, *Reducible polynomials*, J. Lond. Math. Soc. **38** (1963), 183–188.
- [6] S. D. Cohen, *The distribution of the Galois groups of integral polynomials*, Illinois J. Math. **23**(1) (1979), 135–152.
- [7] R. Dietmann, *On the distribution of Galois groups*, Mathematika **58**(1) (2012), 35–44.
- [8] R. Dietmann, *Probabilistic Galois theory*, Bull. London Math. Soc. **45**(3) (2013), 453–462.
- [9] A. Dubickas, *Conjugate algebraic numbers close to a symmetric set*, St. Petersburg Math. J. **16**(6) (2005), 1013–1016.
- [10] A. Dubickas, *On the number of reducible polynomials of bounded naive height*, Manuscripta Math. **144**(3-4) (2014), 439–456.

- [11] A. Dubickas and M. Sha, *Counting degenerate polynomials of fixed degree and bounded height*, Monatsh. Math. **177** (2015), 517–537.
- [12] A. Dubickas and M. Sha, *Counting and testing dominant polynomials*, Exper. Math. **24** (2015), 312–325.
- [13] R. Ferguson, *Irreducible polynomials with many roots of equal modulus*, Acta Arith. **78** (1996/1997), 221–225.
- [14] M. Fujiwara, *Über die obere Schranke des absoluten Betrages der Wurzeln einer algebraischen Gleichung*, Tôhoku Math. J. **10** (1916), 167–171.
- [15] P. X. Gallagher, *The large sieve and probabilistic Galois theory*, In: Analytic number theory (Proceedings of Symposia in Pure Mathematics, vol. 24), pp. 91–101, American Mathematical Society, 1973.
- [16] G. Kuba, *On the distribution of reducible polynomials*, Math. Slovaca **59** (2009), 349–356.
- [17] M. Marden, *Geometry of polynomials*, American Mathematical Society, 1966.
- [18] T. Motzkin, *From among n conjugate algebraic integers, $n - 1$ can be approximately given*, Bull. Amer. Math. Soc. **53** (1947), 156–162.
- [19] M. Sha, *On the decision problems of linear recurrence sequences*, preprint, 2015, <http://arxiv.org/abs/1505.07147>.
- [20] B. L. van der Waerden, *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*, Monatshefte für Matematik und Physik **43** (1936), 133–147.
- [21] M. Waldschmidt, *Diophantine approximation on linear algebraic groups. Transcendence properties of the exponential function in several variables*, Grundlehren der Mathematischen Wissenschaften **326**, Springer, Berlin, 2000.
- [22] D. Zywina, *Hilbert's irreducibility theorem and the larger sieve*, preprint, 2010, <http://arxiv.org/abs/1011.6465>.

DEPARTMENT OF MATHEMATICS AND INFORMATICS, VILNIUS UNIVERSITY,
NAUGARDUKO 24, LT-03225 VILNIUS, LITHUANIA

E-mail address: arturas.dubickas@mif.vu.lt

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF NEW SOUTH WALES, SYDNEY, NSW 2052, AUSTRALIA

E-mail address: shamin2010@gmail.com